UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/595,019	12/16/2005	Johnson Oyama	P18387US2	1263

27045 7590 09/15/2010

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
PHAM, LUU T	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
09/15/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

kara.coffman@ericsson.com
jennifer.hardin@ericsson.com
melissa.rhea@ericsson.com

Office Action Summary	Application No.	Applicant(s)	
	10/595,019	OYAMA, JOHNSON	
	Examiner	Art Unit	
	LUU PHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 June 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *4, 8-14, 16-19, 22, 31-37, 39-41, and 51-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *4, 8-14, 16-19, 22, 31-37, 39-41, and 51-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 0/14/2010 has been entered.

2. As per instant Amendment, Claims 1-3, 5-7, 15, 20-21, 23-30, 38, and 42-50 were previously canceled; Claims 51 and 52 are independent claims. Claims 4, 8-14, 16-19, 22, 31-37, 39-41, and 51-52 have been examined and are pending.

   This Action is made Non-FINAL.

Response to Arguments

3. The objection to the specification as failing to provide proper antecedent basis for the claimed subject matter in claims 51 and 52 is withdrawn as Applicants' arguments are persuasive.

4. The rejections of claims 4, 8-14, 16-19, 22, 31-37, 39-41, and 51-52 under 35 U.S.C. § 112, first paragraph, are withdrawn as Applicants' arguments are persuasive.

5. Applicants' arguments with respect to claims 4, 8-14, 16-19, 22, 31-37, 39-41, and 51-52 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

8. **Claims 4, 8-10, 12-13, 16-17, 19, 31-33, 35-36, 39-40, and 51-52 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Faccin et al., (hereinafter "Faccin '844"), U.S. Patent Application Publication No. 2002/0120844, filed on February 23, 2001, in view of Palekar et al., (hereinafter "Palekar"), U.S. Patent Application Publication No. 2003/0226017, filed on May 30, 2002.

- **Regarding claim 4**, Faccin '844 and Palekar disclose the method of claim 51.

Faccin '844 further discloses transferring MIPv6-related information from the AAA server in the home network to a home agent *(Faccin '884: pars. 0092-0100; Figs. 3-5; AAA-H/AuC 312 sends Km to HA 314).*

- **Regarding claim 8**, Faccin '844 and Palekar disclose the method of claim 51.

Palekar further discloses the protocol for carrying authentication information for network access is an extended Extensible Authentication Protocol (EAP) *(Palekar: pars. 0042 and 0093-0096; Figs. 11-12; the present invention also contemplates the use of an extensible authentication mechanism, such as EAP, through the secure tunnels 601 and 603)* and the MIPv6-related challenge and response messages are incorporated as additional data in the EAP protocol stack *(Palekar: pars. 0093-0098; wherein at least EAP request (identity) 1209; EAP response (user's identify) 1211; EAP request (EAP type=PEAP) 1211; EAP response (EAP type=PEAP) 1215).*

- **Regarding claim 9**, Faccin '844 and Palekar disclose the method of claim 8.

Palekar further discloses MIPv6-related information is transferred in at least one EAP attribute in the EAP protocol stack *(Palekar: pars. 0104-0105; Fig. 13; PEAP packet 310; a length field 1336 that contains the length of the attribute, including the type, length and value fields, and a value field 1338 that contains the value of the name/value pair).*

- **Regarding claim 10**, Faccin '844 and Palekar disclose the method of claim 9.

Palekar further discloses the MIPv6- related information is transferred as EAP attributes of the method layer in the EAP protocol stack *(Palekar: pars. 0060-0061; one*

authentication mechanism which can be selected through the use of EAP is the Transport Layer Security (TLS) protocol; see also pars. 0101-0103; Fig. 13; attempting to negotiate the PEAP protocol).

- **Regarding claim 12**, Faccin '844 and Palekar disclose the method of claim 9.

Palekar further discloses the MIPv6- related information is transferred in a generic container attribute available for any EAP method *(Palekar: pars. 0049-0050; the authenticating server can send an EAP request for a particular authentication protocol, such as CHAP or MS-CHAP; if the user's computing device supports the authentication protocol specified in the EAP request, it can respond with an acknowledgement; see also pars. 0101-0103; Fig. 13; PEAP protocol negotiating process).*

- **Regarding claim 13**, Faccin '844 and Palekar disclose the method of claim 9.

Palekar further discloses the MIPv6- related information is transferred in a method-specific generic container attribute of the method layer in the EAP protocol stack *(Palekar: pars. 0049-0050; the authenticating server can send an EAP request for a particular authentication protocol, such as CHAP or MS-CHAP; if the user's computing device supports the authentication protocol specified in the EAP request, it can respond with an acknowledgement; see also pars. 0101-0103; Fig. 13; PEAP protocol negotiating process).*

- **Regarding claim 16**, Faccin '844 and Palekar disclose the method of claim 4.

Faccin '844 further discloses the MIPv6- related information is transferred from the AAA server in the home network to the home agent in an AAA framework protocol

application *(Faccin '884: pars. 0092-0100; Figs. 3-5; the AAA-H/AuC 312 then chooses a Home Agent and sends the Mobile IP key Km to the selected HA)*.

- **Regarding claim 17**, Faccin '844 and Palekar disclose the method of claim 16.

Faccin '844 further discloses the home agent is a local home agent in the visited network and the MIPv6-related information is transferred from the AAA home server to the local home agent via an AAA server in the visited network *(Faccin '884: pars. 0111-0112; Fig. 5; wherein at least step 522)*.

- **Regarding claim 19**, Faccin '844 and Palekar disclose the method of claim 4.

Faccin '844 further discloses assigning, by the home AAA server, a home agent to the mobile node *(Faccin '884: pars. 0052, 0058-0059, and 0100; The AA-H/AuC 106 then chooses a home agent for the mobile node 100, and sends Mobile IP Key Km to the chosen home agent 108)*; and

distributing by the home AAA server to the mobile node and the home agent, credential-related data for establishing a security association between the mobile node and the home agent *(Faccin '884: pars. 0052, 0058-0059, and 0100; The AA-H/AuC 106 then chooses a home agent for the mobile node 100, and sends Mobile IP Key Km to the chosen home agent 108)*.

- **Regarding claims 31-33**, claims 31-33 are directed to a system associated with the method claimed in claims 8-10. Claims 31-33 are similar in scope to claims 8-10 respectively, and are therefore rejected under similar rationale.

- **Regarding claims 35-36**, claims 35-36 are directed to a system associated with the method claimed in claims 12-13. Claims 35-36 are similar in scope to claims 12-13 respectively, and are therefore rejected under similar rationale.

- **Regarding claims 39-40**, claims 39-40 are directed to a system associated with the method claimed in claims 16-17. Claims 39-40 are similar in scope to claims 16-17 respectively, and are therefore rejected under similar rationale.

- **Regarding claim 51**, Faccin '844 discloses a method of authentication and authorization support for Mobile IP version 6 (MIPv6) *(pars. 0002 and 0011-0013)*, comprising the steps of:

encrypting authentication and authorization information in a mobile node operating in a visited network *(pars. 0030, 0038, 0065, and 0089-0091; Figs. 2 and 3, step 208; MN 200 sends its DH value, encrypted with CK and integrity protected with IK, i.e. CK, IK (DH_ MN))*;

sending the encrypted authentication and authorization information from the mobile node to a [pass-through] Authentication, Authorization and Accounting (AAA) client in the visited network utilizing a protocol for carrying authentication information for network access *(par. 0065; Fig. 2, step 208; the Visited Domain 202 receives the first message but cannot decrypt it since it does not know how to compute Kc, and transmits it to the home domain 204; 'CK,IK(DH_MN)' is known as encrypted authentication and authorization information; pars. 0089-0092; Fig. 3, steps 328-332; the BU is forwarded to the AAA-H)*;

forwarding the encrypted authentication and authorization information from the [pass-through] AAA client to a [pass-through] visited AAA server in the visited network *(par. 0065; Fig. 2, step 208; the Visited Domain 202 receives the first message and transmits it to the home domain 204; pars. 0089-0092; Fig. 3, steps 318 and 330; Fig. 4, steps 418 and 422; the BU is forwarded to the AAA-H)*;

forwarding the encrypted authentication and authorization information from the [pass-through] visited AAA server in the visited network to a home AAA server in the mobile node's home network *(par. 0065; Fig. 2, step 210; the Visited Domain 202 receives the first message and transmits it to the home domain 204; pars. 0089-0092; Figs. 3 and 4, steps 320 and 332; the BU is forwarded to the AAA-H; the AAA-H/AuC 312 verifies the MAC value to make sure the message has not been modified)*;

performing an analysis of the encrypted authentication and authorization information by the home AAA server *(pars. 0066 and 0092-0101; Figs. 3-4; The AAA-H/AuC 312 verifies the MAC value to make sure the message has not been modified)*;

sending a MIPv6-related challenge message from the home AAA server to the mobile node via the [pass-through] visited AAA server and the pass-through AAA client in the visited network based on the analysis of the encrypted authentication and authorization information *(pars. 0068-0069; Fig. 2, steps 212 and 214; the visited domain forwards a message 214 comprising the visited domain DH value encrypted with key CK and integrity protected by IK, compiled by the home domain 201, to the mobile node 200; 'CK,IK(DH_VD)' is considered as 'challenge message contents' since MN, which is the only communication node, is able to decrypt it; see also Fig. 5, steps 522-532)*;

sending a MIPv6-related challenge response message from the mobile node to the home AAA server via the [pass-through] AAA client and the [pass-through] visited AAA server in the visited network *(pars. 0106 and 0108-0112; Fig. 3, steps 352-354; the MN executes a BU with its HA; Fig. 4, step 424; Fig. 5, steps 521-522; the third BU (arrows 424, 426) is a BU with the MN's Home Agent; see also par. 0065; Fig. 2, step 208; the Visited Domain 202 receives the first message and transmits it to the home domain 204; 'CK,IK(DH_MN)' is known as challenge response message contents since home server, which is the only communication node, is able to decrypt it)*;

performing an analysis of the challenge response message contents by the home AAA server *(pars. 0066-0068, 0092-0096, and 0106-0112; Figs. 3-5, the Home network performs authentication the user; the third BU (arrows 424, 426) is a BU with the MN's Home Agent; the AR cannot perform this BU because it does not have the Mobile IP Key)*; and

sending a MIPv6-related authentication and authorization results message from the home AAA server to the mobile node reporting a result of the analysis of the challenge response message contents and providing session parameter information *(pars. 0092-0096, 0106-0112; Figs. 3-5; steps 354, 426, and 532; the MN executes a BU with its HA)*.

Faccin discloses all limitations as recited above, but does not explicitly disclose the AAA client is a pass-through AAA client; and the visited AAA server is a pass-through visited AAA server.

However, in an analogous art, Palekar discloses an authenticating method, wherein the AAA client is a pass-through AAA client and the visited AAA server is a pass-

through visited AAA server *(Palekar: par. 0006; these intermediate points can merely act as a pass-through of EAP packets and do not impact the selection of an authentication protocol; par. 0054; Fig. 6; the foreign access point can act as a pass-through device, simply forwarding along the EAP packets to and from the appropriate foreign authentication server)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Palekar with the method and system of Faccin, wherein the AAA client is a pass-through AAA client and the visited AAA server is a pass-through visited AAA server to provide users with an EAP authentication mechanism, wherein "EAP allows two endpoints to agree on an authentication protocol even if intermediate network points do not understand the selected protocol because these intermediate points can merely act as a pass-through of EAP packets and do not impact the selection of an authentication protocol" *(Palekar: par. 0006)*.

- **Regarding claim 52**, Faccin '844 discloses a system for authentication and authorization support for MIPv6 *(pars. 0002 and 0011-0013)*, comprising:

a mobile node operating in a visited network for encrypting authentication and authorization information and for sending the encrypted authentication and authorization information from the mobile node to a [pass-through] Authentication, Authorization and Accounting (AAA) node in the visited network utilizing a protocol for carrying authentication information for network access *(pars. 0030, 0038, 0065, and 0089-0091; Figs. 2 and 3, step 208; MN 200 sends its DH value, encrypted with CK and integrity*

protected with IK, i.e. CK, IK (DH_ MN); par. 0065; Fig. 2, step 208; the Visited Domain 202 receives the first message but cannot decrypt it since it does not know how to compute Kc, and transmits it to the home domain 204; 'CK,IK(DH_MN)' is known as encrypted authentication and authorization information; pars. 0089-0092; Fig. 3, steps 328-332; the BU is forwarded to the AAA-H);

the [pass-through] AAA node for forwarding [in a pass-through manner] the encrypted authentication and authorization information to a home AAA server in the mobile node's home network *(par. 0065; Fig. 2, step 210; the Visited Domain 202 receives the first message and transmits it to the home domain 204; pars. 0089-0092; Figs. 3 and 4, steps 320 and 332; the BU is forwarded to the AAA-H; the AAA-H/AuC 312 verifies the MAC value to make sure the message has not been modified)*;

the home AAA server for performing an analysis of the encrypted authentication and authorization information *(pars. 0066 and 0092-0101; Figs. 3-4; The AAA-H/AuC 312 verifies the MAC value to make sure the message has not been modified)* and for sending a MIPv6-related challenge message to the mobile node via the [pass-through] AAA node in the visited network based on the analysis of the encrypted authentication and authorization information *(pars. 0068-0069; Fig. 2, steps 212 and 214; the visited domain forwards a message 214 comprising the visited domain DH value encrypted with key CK and integrity protected by IK, compiled by the home domain 201, to the mobile node 200; 'CK,IK(DH_VD)' is considered as 'challenge message contents' since MN, which is the only communication node, is able to decrypt it; see also Fig. 5, steps 522-532)*;

wherein the mobile node sends a MIPv6-related challenge response message to the home AAA server via the [pass-through] AAA node in the visited network *(pars. 0106 and 0108-0112; Fig. 3, steps 352-354; the MN executes a BU with its HA; Fig. 4, step 424; Fig. 5, steps 521-522; the third BU (arrows 424, 426) is a BU with the MN's Home Agent; see also par. 0065; Fig. 2, step 208; the Visited Domain 202 receives the first message and transmits it to the home domain 204; 'CK,IK(DH_MN)' is known as challenge response message contents since home server, which is the only communication node, is able to decrypt it)*; and

wherein the home AAA server performs an analysis of the challenge response message contents by the home AAA server *(pars. 0066-0068, 0092-0096, and 0106-0112; Figs. 3-5, the Home network performs authentication the user; the third BU (arrows 424, 426) is a BU with the MN's Home Agent)*, and sends a MIPv6-related authentication and authorization results message to the mobile node reporting a result of the analysis of the challenge response message contents and providing session parameter information *(pars. 0092-0096, 0106-0112; Figs. 3-5; steps 354, 426, and 532; the MN executes a BU with its HA)*.

Faccin discloses all limitations as recited above, but does not explicitly disclose the Authentication, Authorization, and Accounting (AAA) node is a pass-through node and the pass-through AAA node forwarding information in a pass-through manner.

However, in an analogous art, Palekar discloses an authenticating method, wherein the Authentication, Authorization, and Accounting (AAA) node is a pass-through node *(Palekar: par. 0006; these intermediate points can merely act as a pass-through of*

EAP packets and do not impact the selection of an authentication protocol; par. 0054; Fig. 6; the foreign access point can act as a pass-through device, simply forwarding along the EAP packets to and from the appropriate foreign authentication server); and the pass-through AAA node forwarding information in a pass-through manner *(Palekar: par. 0006; these intermediate points can merely act as a pass-through of EAP packets and do not impact the selection of an authentication protocol; see also par. 0054; Fig. 6)*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Palekar with the method and system of Faccin, wherein the Authentication, Authorization, and Accounting (AAA) node is a pass-through node and the pass-through AAA node forwarding information in a pass-through manner to provide users with an EAP authentication mechanism, wherein "EAP allows two endpoints to agree on an authentication protocol even if intermediate network points do not understand the selected protocol because these intermediate points can merely act as a pass-through of EAP packets and do not impact the selection of an authentication protocol" *(Palekar: par. 0006)*.

9. **Claims 11, 18, 34, and 41 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Faccin in view of Palekar, as applied to claims 51 and 52 above, and further in view of Akhtar et al., (hereinafter "Akhtar"), U.S. Patent No. 7,079,499, filed on September 07, 2000.

- **Regarding claim 11**, Faccin '844 and Palekar disclose the method of claim 10.

Faccin '844 and Palekar do not explicitly disclose the EAP attributes are EAP Type-Length-Value (TLV) attributes.

However, in an analogous art, Akhtar discloses a mobility architecture framework, wherein the EAP attributes are EAP Type-Length-Value (TLV) attributes *(Akhtar: col. 88, lines 4-10; attribute format (AF) that format indicates whether the data attribute follows the type Type/Value (TV) format or follows the Type/Length/Value (TLV) format)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Akhtar with the method and system of Faccin '844 and Palekar, wherein the EAP attributes are EAP Type-Length-Value (TLV) attributes to provide a communication architecture for enabling IP-based mobile communications *(Akhtar: col. 1, lines 56-58)*.

- **Regarding claim 18**, Faccin '844 and Palekar disclose the method of claim 16.

Faccin '844 does not disclose the AAA framework protocol application is an application of a protocol selected from the group of Diameter and RADIUS.

However, in an analogous art, Akhtar discloses a mobility architecture framework, wherein the AAA framework protocol application is an application of a protocol selected from the group of Diameter and RADIUS *(Akhtar: col. 26, lines 1-7; Diameter based AAA with extension for IP mobility is refer, though another AAA protocol such as RADIUS may also be used; see also col. 27, lines 1-5; col. 31, lines 36-42)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Akhtar with the method and system of Faccin '844, wherein the AAA framework protocol application is an application of a protocol selected from the group of Diameter and RADIUS to provide a communication architecture for enabling IP-based mobile communications *(Akhtar: col. 1, lines 56-58)*.

- **Regarding claim 34**, claim 34 is directed to a system associated with the method claimed in claim 11. Claim 34 is similar in scope to claim 11, and is therefore rejected under similar rationale.

- **Regarding claim 41**, claim 41 is directed to a system associated with the method claimed in claim 18. Claim 41 is similar in scope to claim 18, and is therefore rejected under similar rationale.

10. **Claims 14 and 37 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Faccin in view of Palekar, as applied to claims 51 and 52 above, and further in view of Ohba et al., (hereinafter "Ohba"), U.S. Patent Application Publication No. 2004/0098588, filed on July 01, 2003.

- **Regarding claim 14**, Faccin '844 and Palekar disclose the method of claim 51.

Faccin '844 and Palekar do not explicitly disclose the protocol for carrying authentication information for network access is selected from the group of the Protocol for carrying Authentication for Network Access (PANA), IEEE 802.1X, and Point-to-Point Protocol (PPP).

However, in an analogous art, Ohba discloses an authentication method, wherein the protocol for carrying authentication information for network access is selected from the group of the Protocol for carrying Authentication for Network Access (PANA), IEEE 802.1X, and Point-to-Point Protocol (PPP) *(Ohba: par. 0008 and 0034-0035; EAP supports PPP network access authentication; however, EAP may also support other network access authentication methods such as IEEE 802.1X or PANA).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings Ohba with the method and system of Faccin and Palekar, wherein the protocol for carrying authentication information for network access is selected from the group of the Protocol for carrying Authentication for Network Access (PANA), IEEE 802.1X, and Point-to-Point Protocol (PPP) to provide users with an authentication method wherein EAP supports not only for PPP protocol but

also for PANA and 802.1X for fast authentication of a communication session *(Ohba: par. 0034)*.

- **Regarding claim 37**, claim 37 is directed to a system associated with the method claimed in claim 14. Claim 37 is similar in scope to claim 14, and is therefore rejected under similar rationale.

11. **Claim 22 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Faccin, as applied to claims 51 and 52 above, in view of Faccin et al., (hereinafter "Faccin_Internet-Draft"), "Diameter Mobile IPv6 Application, draft-le-aaa-diameter-mobileipv6-6-03.txt," Internet Draft, XP015004098, published in April 2003.

- **Regarding claim 22**, Faccin '844 and Palekar disclose the method of claim 19.

Faccin '844 and Palekar do not explicitly disclose building, at the mobile node, a home address for the mobile node using at least a portion of the address of its assigned home agent; and transferring the home address of the mobile node from the mobile node to the AAA home network server using around trip of a selected EAP procedure.

However, in an analogous art, Faccin_Internet-Draft discloses a Mobile IPv6 document, including steps of building, at the mobile node, a home address for the mobile node using at least a portion of the address of its assigned home agent *(Faccin_Internet-Draft: page 12, section 7.3.1; pages 15-16, section 7.6; page 20-21, section 9.2.1; the home address option set to the NM home address)*; and transferring the home address of the mobile node from the mobile node to the AAA home network server using around trip of a

selected EAP procedure *(Faccin_Internet-Draft: page 12, section 7.3.1; page 2-21, section 9.2.1; if the MN already has a home address and a home agent, it can send a Home Binding Update together with the request to be authorized and authenticated to save one round trip over the access link)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Faccin_Internet-Draft with the method and system of Faccin and Palekar to include steps of building, at the mobile node, a home address for the mobile node using at least a portion of the address of its assigned home agent; and transferring the home address of the mobile node from the mobile node to the AAA home network server using around trip of a selected EAP procedure to enable Mobile IPv6 roaming in networks other than its home *(Faccin_Internet-Draft: page i, abstract)*.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2437